COMMENTS ON THE NATIONAL BROADBAND PLAN
RECOMMENDATION TO CREATE A CYBER SECURITY ROADMAP

What are the most vital cyber security vulnerabilities for communication networks or users?

Absence of:

1. Risk Management
2. Availability Management
3. Integrity Management
4. Contingency Management
5. Penalties for Lack of Compliance

How can these vulnerabilities be addressed?

1. Require the identification and documentation of the Critical Communication Assets that support the reliable operation of the Bulk Electric System through a risk-based assessment.

2. Require the Critical Communication Assets responsible for delivering, storing and processing information are accessible when needed to support the reliable operation of the Bulk Electric System.

3. Require the Critical Communication Assets that support the reliable operation of the Bulk Electric System be secure, can be trusted and relied upon.

4. Require the Critical Communication Assets Contingency Plans, that support the reliable operation of the Bulk Electric System, be thoroughly tested.

5. Require Commission audits with the potential for significant penalties for lack of controls compliance that could negatively impact the reliable operation of the Bulk Electric System.

What roll should the Commission play in addressing them?

Develop Critical Cyber Security Communications Requirements similar to the format used for NERC/CIP for the Bulk Electric System.

What steps should the Commission take, if any, to remediate them?

- Develop Critical Cyber Security Communications Requirements;
- Increase the volume of dedicated networks;
- Implement risk-assessments and background check requirements for personnel working on Critical Cyber Security Communications Requirements;
- Expand Cyber Security Communications education.